Transfer Risk Assessment

1. Purpose

Some of Subcontext's sub-processors process personal data in the United States. This assessment records how those restricted transfers are made lawful under the UK GDPR, and why the data remains adequately protected.

It follows the approach in the Information Commissioner's Office guidance on transfer risk assessments: describing the transfers, assessing the risk of harm to individuals from the data being transferred, considering the protections offered by the destination's legal regime and by the transfer mechanism, and reaching an overall conclusion. Customers can rely on it when considering their own obligations as controllers.

2. Scope and Background

- **Restricted transfer:** under the UK GDPR, a transfer of personal data to a recipient outside the UK is restricted unless the destination is covered by UK adequacy regulations. Transfers to the European Economic Area, including AWS in Ireland and Meta in Ireland, are covered by UK adequacy regulations and are not restricted
- **When an assessment is needed:** an assessment is required where a transfer relies on the International Data Transfer Agreement or the UK Addendum. It is not required for transfers to US recipients certified under the UK Extension to the EU-US Data Privacy Framework, which rely on UK adequacy regulations. This assessment covers all US transfers for completeness, whichever mechanism applies
- **Roles:** Subcontext is the exporter as processor for customer data, and as controller for its own users' and contacts' data

3. Transfers in Scope

Sub-processor	Purpose	Data
Amazon Web Services	Hosting support services and email delivery	Customer data
OpenAI	Speech and conversation for voice calls	Call audio, conversation content
ElevenLabs	Speech synthesis for voice calls	Agent response text
Twilio	SMS, WhatsApp and voice delivery	Phone numbers, message content, call audio
Stripe	Payment processing	Billing and payment data
Meta Platforms	WhatsApp messaging, ads conversion reporting where connected	Phone numbers, message content, hashed contact details

Sub-processor	Purpose	Data
Google	Calendar, Sheets and ads conversion reporting where connected; Android push and crash reporting	Booking details, hashed contact details, device data
Apple	Push notifications to Subcontext's apps	Device tokens, notification content
Persona (via Twilio)	Identity checks for phone number registration	Customer representatives' identity data

Text conversations with AI agents are processed in the UK and EU, and are not part of these transfers.

Primary storage of customer data is in the AWS Ireland (eu-west-1) region. Text AI runs on AWS Bedrock in the EU (Ireland, whose EU cross-region routing may serve a request from another AWS EU region) and London, and requests to US-routed models are refused.

4. Transfer Mechanisms

- Where the recipient is certified under the UK Extension to the EU-US Data Privacy Framework, transfers rely on the UK-US data bridge
- Otherwise, transfers are made under the UK International Data Transfer Agreement, or the EU Standard Contractual Clauses with the UK Addendum

The mechanism relied on for each sub-processor is confirmed during supplier due diligence under the Supplier Risk Management Policy, and checked again at each review, including whether the recipient's certification remains active.

5. Risk of Harm to Individuals

The ICO approach first considers how much harm individuals could suffer if the transferred data were accessed by a third party, including a public authority, without proper safeguards.

Transfer	Data and its sensitivity	Who it relates to	Harm risk
AWS (US services, email delivery)	Customer data in transit through supporting services and email	Customers' customers, platform users	Moderate
OpenAI and ElevenLabs	Call audio and conversation content for voice calls, which may include details needed for a quote	Customers' customers who use voice	Moderate
Twilio	Phone numbers, message content and call audio	Customers' customers	Moderate
Stripe	Billing and payment data; card details are handled by Stripe and never stored by Subcontext	Customers and their customers making payments	Moderate
Meta Platforms	Phone numbers and WhatsApp message content; hashed contact details for ads reporting	Customers' customers	Moderate for messaging, low for hashed data
Google	Booking details, sheet rows, hashed contact details, device data	Customers' customers, platform users	Low

Transfer	Data and its sensitivity	Who it relates to	Harm risk
Apple	Device tokens and notification content	Platform users	Low
Persona (via Twilio)	Identity data of customers' business representatives	Named individuals at customer firms	Moderate

Special category data, such as health information collected for an insurance application, is analysed by AI in the UK and EU, not in the US. It may still appear in message content carried by Twilio or Meta, or be spoken on a voice call, so those transfers are treated as moderate risk and voice data is limited to customers who use voice.

6. Assessment of the Destination

US law gives authorities powers to request data for national security purposes. Executive Order 14086 introduced limits on those powers and a redress mechanism for UK individuals, which underpins the UK-US data bridge. The data in scope is mostly operational (message delivery, payments, speech for calls), and is of low interest to such authorities.

In line with the ICO approach, Subcontext considers:

- **Enforceability of the transfer mechanism:** the IDTA, the Standard Contractual Clauses with the UK Addendum, and Data Privacy Framework commitments are enforceable contractual or regulatory commitments by established companies, and the US has a functioning court system able to enforce contracts
- **Third-party access:** the main concern is access by US public authorities for national security purposes. Executive Order 14086 requires such access to be necessary and proportionate, and provides a redress route through the Data Protection Review Court, which the UK government took into account when making the UK-US data bridge
- **Likelihood in practice:** the recipients are commercial service providers, and the data is transactional and short-lived in most cases. Large providers publish transparency reports on government requests

7. Supplementary Measures

- All data is encrypted in transit, and at rest by the providers
- Only the data needed for each task is sent
- Contact details used for ads reporting are hashed before they are sent
- Voice data goes to the US only for voice calls, and only for customers who use voice
- Providers' commitments not to use the data to train models, and their transparency reports, are reviewed as part of supplier due diligence

Further measures that support the assessment:

- OpenAI does not train on API data and may retain it for up to 30 days for abuse monitoring
- Each customer's messaging can run in its own isolated Twilio account
- Credentials for sub-processors are encrypted at rest, and callbacks from them are signature-verified
- Sub-processor agreements require prompt notification of personal data breaches and flow down equivalent obligations to their own sub-processors

8. Conclusion

With these mechanisms and measures, the transferred data receives protection that is not materially lower than in the UK, and the transfers may continue.

Transfer	Conclusion
All transfers in section 3	May proceed under the mechanism recorded for each sub-processor

9. Monitoring and Triggers for Reassessment

This assessment is revisited, in addition to the regular review, if:

- A sub-processor loses its Data Privacy Framework certification, or the UK-US data bridge is withdrawn or challenged
- US law on public authority access to data changes significantly
- A sub-processor reports a government request or breach affecting Subcontext data
- A new type of data, especially special category data, starts to be sent to a US recipient

If a transfer can no longer be justified, Subcontext will consider switching to a UK or EU region or provider, suspending the feature that relies on it, and telling affected customers.

10. Review

This assessment is reviewed at least annually, when a new sub-processor outside the UK is engaged, and when the relevant law changes.

11. Related Documents

- Sub-Processor List
- Supplier Risk Management Policy
- Data Protection Impact Assessment
- Encryption & Key Management Policy
- Data Retention & Deletion Policy

12. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, when a new sub-processor outside the UK is engaged, and when the relevant law changes
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.